

Implementación de Endian (EFW) en VM

Duvan Steven Espitia Barrios
e-mail: dseb@unadvirtual.edu.co

Resumen— Este artículo detalla la configuración e implementación de una instancia de GNU/Linux Endian como firewall dentro de un entorno VirtualBox, cubriendo los pasos esenciales para la asignación estratégica de las tarjetas de red a las zonas de seguridad (verde/LAN, roja/WAN y naranja/DMZ). Este proceso es fundamental para lograr una segmentación de red efectiva y segura, culminando en una solución de cortafuegos robusta y lista para ser utilizada tanto en entornos de producción como de prueba.

Palabras clave: Virtual box, Máquina Virtual, Firewall, Endian, Red, GNU/LINUX

I. Introducción

En este trabajo se implementó un Proxy HTTP no transparente utilizando la distribución Endian Firewall (EFW) con el propósito de controlar el acceso a Internet y aplicar políticas de seguridad sobre la red LAN. Se configuraron perfiles de filtrado, autenticación por usuario y listas negras de navegación, verificando su funcionamiento desde un cliente Linux en la red interna. Esta práctica demuestra el uso de Endian como solución de seguridad para la gestión y protección del tráfico en redes empresariales.

II. Desarrollo de Contenidos

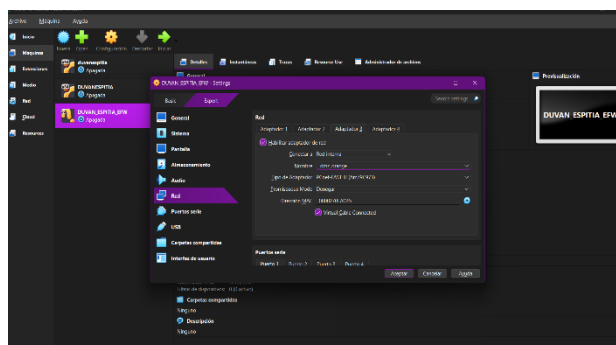
A partir de esta sección, se desarrollan los contenidos de la actividad, de una forma ordenada y secuencial. Para este caso se inicia con los requisitos para instalación de Endian EFW

A. Requisitos de Instalación

Se requirió del uso de la máquina virtual “virtual box”, Imagen ISO de Endian EFW, 2Gb de Ram, 4 Nucleos para el procesador, Memoria de 50Gb

Configuración previa: Endian necesita 3 adaptadores con funciones diferentes antes de iniciarlo así: Adaptador 1 WAN (RED), Adaptador 2 GREEN (LAN), Adaptador 3 ORANGE (DMZ)

Figura 1: Configuración previa para la instalación de Endian EFW



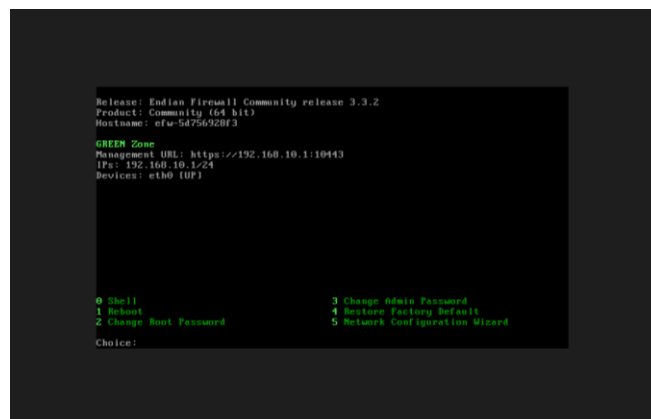
Fuente: Elaboración propia

B. Instalación Endian EFW

La instalación de Endian Firewall (EFW) se realizó en un entorno

virtualizado mediante VirtualBox, configurando una máquina virtual dedicada con tres interfaces de red para operar como firewall entre los segmentos WAN, LAN y DMZ. Durante el asistente de instalación se seleccionó la interfaz GREEN (LAN) como red interna principal y se asignó la dirección 192.168.10.1/24, la cual permitió posteriormente el acceso a la consola web de administración. Una vez completado el proceso de instalación, se establecieron las contraseñas administrativas y se verificó la comunicación desde un cliente Ubuntu Desktop configurado con la dirección 192.168.10.10, puerta de enlace 192.168.10.1 y DNS público 8.8.8.8. Esta configuración inicial habilitó la gestión remota de EFW, permitiendo la activación de servicios adicionales como el proxy HTTP, políticas de autenticación y filtrado de tráfico, fundamentales para su rol como dispositivo de seguridad en la infraestructura de red.

Figura 2: Instalación correcta Endian EFW

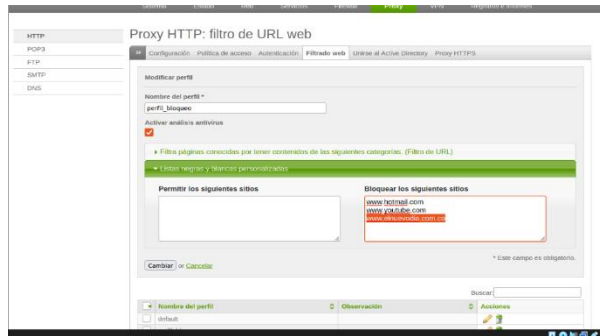


Fuente: Elaboración propia

C. Configuración de Endian EFW

Tras la instalación inicial, la configuración de Endian Firewall (EFW) se realizó mediante su interfaz web de administración accedida desde la red GREEN (<http://192.168.10.1>). Desde este panel se habilitó el servicio de Proxy HTTP en modo no transparente, asignando el puerto estándar 8080 y activando la autenticación basada en usuarios NCSA. Se creó un grupo de acceso y un usuario asociado y posteriormente se definió un perfil de filtrado con una lista negra que incluía los dominios *youtube.com*, *hotmail.com* y *elnuevodia.com.co*. Este perfil fue vinculado a la política de acceso del proxy, junto con la política de autenticación correspondiente. Finalmente, se importó en el cliente Ubuntu Desktop el certificado HTTPS generado por Endian, permitiendo la inspección SSL y habilitando el bloqueo efectivo, de los sitios configurados. Esta configuración integró control de acceso, filtrado web y autenticación centralizada para la gestión segura del tráfico LAN hacia la WAN

Figura 3: Configuración Endia EFW

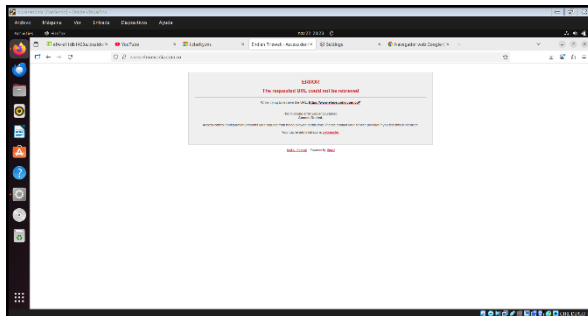


Fuente: Elaboración propia

D. Validación del Funcionamiento del Proxy y las Políticas de Filtrado

Se evaluó el correcto funcionamiento del proxy HTTP configurado en Endian Firewall desde un cliente ubicado en la red LAN. Para ello, se utilizó un equipo Ubuntu Desktop con la configuración de red establecida y el proxy asignado manualmente en el navegador web. Al acceder a cualquier sitio de Internet, el navegador solicitó las credenciales del usuario previamente creado en Endian, validando así la autenticación NCSA; una vez, acreditado el usuario, se procedió a probar los dominios incluidos en la lista negra (youtube.com, hotmail.com y elnuevodia.com.co), verificando que todos fueran efectivamente bloqueados. Este proceso confirmó la correcta operación del proxy, la aplicación del perfil de filtrado y la funcionalidad de las políticas de autenticación configuradas, garantizando el control y restricción del tráfico HTTP/HTTPS desde la red LAN

Figura 4: Filtrado WEB



Fuente: Elaboración propia

III. Conclusiones

La implementación de Endian Firewall permitió establecer un entorno de seguridad funcional en el que la autenticación de usuarios, el filtrado web y el control de acceso se integraron de manera efectiva para proteger la red LAN. La configuración del proxy HTTP no transparente, junto con la creación de perfiles de bloqueo y listas negras, aseguró la restricción eficiente de sitios no autorizados, mientras que las pruebas desde el cliente Ubuntu confirmaron el correcto funcionamiento de las políticas aplicadas. En conjunto, el proceso demostró la capacidad de Endian para gestionar de forma confiable el tráfico web y reforzar la seguridad en infraestructuras basadas en GNU/Linux.

IV. Reconocimientos

Los autores agradecen el apoyo brindado por la institución académica UNAD y por las herramientas proporcionadas para el desarrollo de este taller, especialmente el uso de entornos virtualizados y plataformas GNU/Linux que permitieron reproducir de manera controlada la arquitectura de red empleada; así mismo, se reconoce el valor educativo del uso de Endian Firewall como solución práctica para comprender los fundamentos de seguridad, filtrado de contenido y gestión de tráfico en infraestructuras de red modernas

V. Referencias

- [1] Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. <https://help.ubuntu.com/20.04/ubuntu-help/index.html>
- [2] Oracle (2020). Endian UTM 3.2 Manual referencia. Endian. <http://docs.endian.com/3.2/utm/index.html>
- [3] Debian (2023). El manual del administrador de Debian Manual de usuario VirtualBox. VirtualBox. <https://www.virtualbox.org/manual>
- [4] Endian (2016), <https://www.debian.org/releases/stable/amd64/index.es.html>
- [5] Jay LaCroix. (2020). Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server. Packt Publishing. <https://research-ebSCO-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952>